WHAT IS CLAIMED IS:

1. A method for detecting unauthorized access of a cable system by a cable modem auxiliary device (CMAD), the method comprising:

receiving at a cable modem termination system (CMTS) a DHCP request from a CMAD seeking access to the cable system, the DHCP request comprising a MAC address of the CMAD and a MAC address of a cable modem to which the CMAD is connected;

forming a proffered identifier of the CMAD by combining the gateway interface address of the CMTS with the CMAD MAC address and the cable modem MAC address; and

storing the proffered identifier in a data store.

2. The method for detecting unauthorized access of a cable system by a CMAD of claim 1, wherein the CMAD comprises a media terminal adapter.

3. The method for detecting unauthorized access of a cable system by a CMAD of claim 1, wherein the CMAD comprises a set top box.

4. The method for detecting unauthorized access of a cable system by a CMAD of claim 1, wherein the CMAD is integrated with a cable modem.

5. The method for detecting unauthorized access of a cable system by a CMAD of claim 1, wherein the datastore comprises a central database.

6. The method for detecting unauthorized access of a cable system by a CMAD of claim 1, wherein the datastore comprises a distributed database.

7. A method for detecting unauthorized access of a cable system by a cable modem auxiliary device (CMAD), the method comprising:

receiving at a cable modem termination system (CMTS) a DHCP request comprising a MAC address of a CMAD seeking access to the cable system and a MAC address of a cable modem (CM) to which the CMAD is connected;

forming a proffered identifier of the CMAD by combining a gateway interface address of the CMTS with the CM MAC address and the CMAD MAC address;

comparing the components of the proffered identifier to the components of each of one or more stored identifiers stored in a datastore;

making a determination whether the proffered identifier and any of the one or more stored identifiers satisfy a matching criteria comprising a same CMAD MAC address component and a different gateway interface address component; and

in the event the proffered identifier and any of the one or more stored identifiers satisfy the matching criteria, selecting a remedial response.

8. The method for detecting unauthorized access of a cable system by a CMAD of claim 7, wherein the datastore comprises a central database.

9. The method for detecting unauthorized access of a cable system by a CMAD of claim 7, wherein the datastore comprises a distributed database.

10. The method for detecting unauthorized access of a cable system by a CMAD of claim 7, wherein the cable system comprises a DHCP server linked to the CMTS and wherein the DHCP server makes the determination with respect to the matching criteria.

11. The method for detecting unauthorized access of a cable system by a CMAD of claim 7, wherein the remedial response comprises denying the CMAD access to the cable system, sending an advisory message to a network manager, and recording the event in a log file.

12. A method for detecting unauthorized access of a cable system by a CMAD, wherein the method comprises:

receiving at a cable modem termination system (CMTS) a DHCP request comprising a MAC address of a CMAD seeking access to the cable system and a MAC address of a cable modem (CM) to which the CMAD is connected;

forming a proffered identifier of the CMAD by combining a gateway interface address of the CMTS with the CM MAC address and the CMAD MAC address;

comparing the components of the proffered identifier to the components of each of one or more stored identifiers stored in a datastore;

making a determination whether the proffered identifier and any of the one or more stored identifiers satisfies a matching criteria comprising a same CMAD MAC address

component, a different CM MAC address component, and a same gateway interface address component; and

in the event the proffered identifier and any of the one or more stored identifiers satisfy the matching criteria, selecting a remedial response.

13. The method for detecting unauthorized access of a cable system by a CMAD of claim 12, wherein the datastore comprises a central database.

14. The method for detecting unauthorized access of a cable system by a CMAD of claim 12, wherein the datastore comprises a distributed database.

15. The method for detecting unauthorized access of a cable system by a CMAD of claim 12, wherein the cable system further comprises a DHCP server linked to the CMTS and wherein the DHCP server makes the determination with respect to the matching criteria.

16. The method for detecting unauthorized access of a cable system by a CMAD of claim 12, wherein the remedial response comprises denying the CMAD access to the cable system, sending an advisory message to a network manager, and recording the event in a log file.

17. A method for detecting unauthorized access of a cable system by a cable modem auxiliary device (CMAD), the method comprising:

receiving at a cable modem termination system (CMTS) a DHCP request comprising a MAC address of a CMAD seeking access to the cable system and a MAC address of a cable modem (CM) to which the CMAD is connected;

forming a proffered identifier of the CMAD by combining a gateway interface address of the CMTS with the CM MAC address and the CMAD MAC address;

comparing the components of the proffered identifier to the components of each of one or more stored identifiers stored in a datastore;

making a first determination whether the proffered identifier and any of the one or more stored identifiers satisfy a first matching criteria comprising a same CMAD MAC address component and a different gateway interface address component;

in the event the proffered identifier and any of the one or more stored identifiers satisfy the first matching criteria, selecting a remedial response;

in the event the proffered identifier and any of the one or more stored identifiers do not satisfy the first matching criteria, making a second determination whether the proffered identifier and any of the one or more stored identifiers satisfies a second matching criteria comprising a same CMAD MAC address component, a different CM MAC address component, and a same gateway interface address component; and

in the event the proffered identifier and any of the one or more stored identifiers satisfy the second matching criteria, selecting a remedial response.

18. The method for detecting unauthorized access of a cable system by a CMAD of claim 17, wherein the datastore comprises a central database.

19. The method for detecting unauthorized access of a cable system by a CMAD of claim 17, wherein the datastore comprises a distributed database.

20. The method for detecting unauthorized access of a cable system by a CMAD of claim 17, wherein the cable system further comprises a DHCP server linked to the CMTS and wherein the DHCP server makes the determination with respect to the first matching criteria and the determination with respect to the second matching criteria.

21. The method for detecting unauthorized access of a cable system by a CMAD of claim 17, wherein the remedial response comprises denying the CMAD access to the cable system, sending an advisory message to a network manager, and recording the event in a log file.

22. The method for detecting unauthorized access of a cable system by a CMAD of claim 17, wherein the method further comprises in the event that the proffered identifier and any of the one or more stored identifiers do not satisfy the first matching criteria and the second matching criteria, storing the proffered identifier in the datastore.

23. A method for detecting unauthorized access of a cable system by a cable modem auxiliary device (CMAD), wherein the cable system comprises a plurality of regional cable networks each having a regional datastore, the method comprising:

receiving at a cable modem termination system (CMTS) a DHCP request comprising a MAC address of a CMAD seeking access to one of the plurality of regional cable networks and a MAC address of a cable modem (CM) to which the CMAD is connected;

forming a proffered identifier of the CMAD by combining a gateway interface address of the CMTS with the proffered CM MAC address and the proffered CMAD MAC address;

comparing the components of the proffered identifier to the components of each of one or more stored identifiers stored in a regional datastore;

making a first determination whether the proffered identifier and any of the one or more regionally stored identifiers satisfy a first matching criteria comprising a same CMAD MAC address component and a different gateway interface address component;

in the event the proffered identifier and any of the one or more regionally stored identifiers satisfy the matching criteria, selecting a remedial response;

in the event the proffered identifier and any of the one or more regionally stored identifiers do not satisfy the first matching criteria, making a second determination whether the proffered identifier and any of the one or more regionally stored identifiers satisfies a second matching criteria comprising a same CMAD MAC address component, a different CM MAC address component, and a same gateway interface address component;

in the event the proffered identifier and any of the one or more regionally stored identifiers satisfy the second matching criteria, selecting a remedial response;

in the event that the proffered identifier and any of the one or more regionally stored identifiers do not satisfy the first matching criteria and the second matching criteria, comparing the components of the proffered identifier to the components of each of one or more stored identifiers stored in a central datastore, wherein the central datastore comprises regionally stored identifiers from each of the regional datastores;

making a third determination whether the proffered identifier and any of the one or more centrally stored identifiers satisfy the first matching criteria comprising;

in the event the proffered identifier and any of the one or more centrally stored identifiers satisfy the first matching criteria, selecting a remedial response;

in the event the proffered identifier and any of the one or more centrally stored identifiers do not satisfy the first matching criteria, making a fourth determination whether the

proffered identifier and any of the one or more centrally stored identifiers satisfies the second matching criteria; and

in the event the proffered identifier and any of the one or more centrally stored identifiers satisfy the second matching criteria, selecting a remedial response.

24. The method for detecting unauthorized access of a cable system by a CMAD of claim 23, wherein the regional datastore and the central datastore each comprise a central database.

25. The method for detecting unauthorized access of a cable system by a CMAD of claim 23, wherein the regional datastore and the central datastore each comprise a distributed database.

26. The method for detecting unauthorized access of a cable system by a CMAD of claim 23, wherein at least one of the plurality of regional cable networks further comprises a DHCP server linked to the CMTS and wherein the DHCP server makes the first determination and the second determination.

27. The method for detecting unauthorized access of a cable system by a CMAD of claim 23, wherein the remedial response comprises denying the CMAD access to the cable system, sending an advisory message to a network manager, and recording the event in a log file.

28. The method for detecting unauthorized access of a cable system by a CMAD of claim 23, wherein the method further comprises in the event that the proffered identifier and any of the one or more centrally stored identifiers do not satisfy the first matching criteria and the second matching criteria, storing the proffered identifier in the regional datastore and the central datastore.

29. A method for detecting unauthorized access of a cable system by a cable modem auxiliary device (CMAD), the method comprising:

receiving a DHCP request comprising a MAC address of a CMAD seeking access to the cable system;

comparing the components of the proffered CMAD MAC address to each of one or more stored rejected CMAD MAC addresses in a datastore;

determining whether the proffered CMAD MAC address and any of the one or more rejected CMAD MAC addresses are related; and

in the event the proffered CMAD MAC address and any of the one or more CMAD MAC addresses stored in the datastore are related, selecting a remedial response.

30. The method for detecting unauthorized access of a cable system by a CMAD of claim 29, wherein determining whether the proffered CMAD MAC address and any of the one or more of the rejected CMAD MAC addresses are related comprises determining whether the proffered CMAD MAC address any of the one or more of the rejected CMAD MAC addresses are related temporally.

31. The method for detecting unauthorized access of a cable system by a CMAD of claim 29, wherein determining whether the proffered CMAD MAC address and any of the one or more of the rejected CMAD MAC addresses are related comprises determining whether the proffered CMAD MAC address any of the one or more of the rejected CMAD MAC addresses are related sequentially.

32. The method for detecting unauthorized access of a cable system by a CMAD of claim 29, wherein determining whether the proffered CMAD MAC address and any of the one or more of the rejected CMAD MAC addresses are related comprises determining whether the proffered CMAD MAC address any of the one or more of the rejected CMAD MAC addresses are related by manufacturer code.

33. The method for detecting unauthorized access of a cable system by a CMAD of claim 29, wherein the datastore comprises a central database.

34. The method for detecting unauthorized access of a cable system by a CMAD of claim 29, wherein the datastore comprises a distributed database.

35. The method for detecting unauthorized access of a cable system by a CMAD of claim 29, wherein the remedial response comprises identifying the location of the CMAD seeking to access the cable system, sending an advisory message to a network manager, and recording the event in a log file.

36. A system for detecting unauthorized access of a cable network by a cable modem, auxiliary device (CMAD) the system comprising:

a CMTS adapted to:

receive a DHCP request comprising a MAC address of a CMAD seeking access to the cable system and a MAC address of a cable modem (CM) to which the CMAD is connected; and

form a proffered identifier by combining a gateway interface address of the CMTS with the CM MAC address and the CMAD MAC address; and

a detection server linked to a datastore, the detection server adapted to:

receive the proffered identifier from the CMTS;

compare the components of the proffered identifier to the components of each of one or more stored identifiers stored in the datastore;

determine whether the proffered identifier and any of the one or more stored identifiers satisfy a first matching criteria comprising a same CMAD MAC address component and a different gateway interface address component; and

in the event the proffered identifier and any of the one or more stored identifiers satisfy the first matching criteria, select a remedial response.

37. The system of claim 36, wherein the detection server is further adapted to:

determine whether the proffered identifier and any of the one or more stored identifiers satisfies a second matching criteria comprising a same CMAD MAC address component, a different CM MAC address component, and a same gateway interface address component; and

in the event the proffered identifier and any of the one or more stored identifiers satisfy the second matching criteria, select a remedial response.

38. The system of claim 36, wherein the detection server is further adapted to in the event the proffered identifier and any of the one or more stored identifiers do not satisfy the first matching criteria and the second matching criteria, store the proffered identifier in the datastore.

39. The system of claim 36, wherein the datastore comprises a central database.

40. The system of claim 36, wherein the datastore comprises a distributed database.

41. The system of claim 36, wherein the remedial response comprises denying the CMAD access to the cable system, sending an advisory message to a network manager, and recording the event in a log file.

42. The system of claim 36, wherein the detection server comprises a DHCP server.

43. A system for detecting unauthorized access of a cable network comprising a plurality of regional cable networks by a cable modem auxiliary device (CMAD), the system comprising:

a CMTS adapted to:

receive a DHCP request comprising a MAC address of a CMAD seeking access to one of the plurality of regional cable networksand a MAC address of a cable modem (CM) to which the CMAD is connected; and

form a proffered identifier by combining a gateway interface address of the CMTS with the CM MAC address and the CMAD MAC address; and

a regional detection server linked to a regional datastore, the regional detection server adapted to:

receive the proffered identifier from the CMTS;

compare the components of the proffered identifier to the components of each of one or more stored identifiers stored in the regional datastore;

determine whether the proffered identifier and any of the one or more regionally stored identifiers satisfy a first matching criteria comprising a same CMAD MAC address component and a different gateway interface address component;

in the event the proffered identifier and any of the one or more regionally stored identifiers satisfy the first matching criteria, select a remedial response;

in the event the proffered identifier and any of the one or more regionally stored identifiers do not satisfy the first matching criteria, determine whether the proffered identifier and any of the one or more regionally stored identifiers satisfies a second matching criteria comprising a same CMAD MAC address component, a different CM MAC address component, and a same gateway interface address component;

in the event the proffered identifier and any of the one or more regionally stored identifiers satisfy the second matching criteria, select a remedial response;

in the event that the proffered identifier and any of the one or more regionally stored identifiers do not satisfy the first matching criteria and the second matching criteria, send the proffered identifier to a central detection server; and

the central detection server linked to a central datastore, the central detection server adapted to:

compare the components of the proffered identifier to the components of each of one or more stored identifiers stored in a central datastore, wherein the central datastore comprises regionally stored identifiers from each of the regional datastores;

determine whether the proffered identifier and any of the one or more centrally stored identifiers satisfy the first matching criteria;

in the event the proffered identifier and any of the one or more centrally stored identifiers satisfy the first matching criteria, select a remedial response;

in the event the proffered identifier and any of the one or more centrally stored identifiers do not satisfy the first matching criteria, determine whether the proffered identifier and any of the one or more centrally stored identifiers satisfies the second matching criteria; and

in the event the proffered identifier and any of the one or more centrally stored identifiers satisfy the second matching criteria, select a remedial response.

44. The system of claim 43, wherein the central detection server is further adapted to in the event the proffered identifier and any of the one or more centrally stored identifiers do not satisfy the first matching criteria and the second matching criteria, store the proffered identifier in the regional datastore and the central datastore.

45. The system of claim 43, wherein the regional datastore and the central datastore each comprise a central database.

46. The system of claim 43, wherein the regional datastore and the central datastore each

comprise a distributed database.

47. The system of claim 43, wherein the remedial response comprises denying the CMAD access to the cable system, sending an advisory message to a network manager, and recording the event in a log file.

48. The system of claim 43, wherein the regional detection server comprises a DHCP server.

49. A method for detecting unauthorized access of a cable system by a cable network device (CND), the method comprising:

receiving at a cable modem termination system (CMTS) a DHCP request from a CND seeking access to the cable system, wherein the DHCP request comprises a MAC address;

forming a proffered identifier by combining the gateway interface address of the CMTS with the proffered MAC address;

comparing the proffered identifier to preauthorized identifiers in a datastore;

in the event the proffered identifier matches a preauthorized identifier, granting the CND temporary access to the cable system;

requesting from the CND a confirmation identifier; and

in the event the confirmation identifier is received from the CND, granting the CND access to the cable system.

50. The method for detecting unauthorized access of a cable system by a CND of claim 49, the method further comprising in the event the proffered identifier does not matches a preauthorized identifier, selecting a remedial response.

51. The method for detecting unauthorized access of a cable system by a CND of claim 49, the method further comprising in the event the confirmation identifier is not received, terminating the temporary access to the cable system.